

```

(afl_env) (base) user@ubuntu:~/zgd/AFLProject/pdf_parsers/mupdf-1.25.6-source/build$ ./debug/mutool clean ../../../../p
df_fuzz/mupdf-1.25.5-source/mutool/clean/analyze_crashes/mupdf-clean-poc /dev/null
warning: unknown PDF version: 0.-6
format error: cannot recognize xref format
warning: trying to repair broken xref
warning: repairing PDF document
warning: invalid indirect reference in dict
syntax error: invalid key in dict
warning: invalid indirect reference in dict
syntax error: invalid key in dict
warning: ignoring broken object (3 0 R)
warning: skipping invalid page range
Segmentation fault (core dumped)

```

```

(afl_env) (base) user@ubuntu:~/zgd/AFLProject/pdf_parsers/mupdf-1.25.6-source/build$ ls
core.2323265 debug
(afl_env) (base) user@ubuntu:~/zgd/AFLProject/pdf_parsers/mupdf-1.25.6-source/build$ gdb ./debug/mutool core.2323265
GNU gdb (Ubuntu 12.1-0ubuntu1~22.04.2) 12.1
Copyright (C) 2022 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
--Type <RET> for more, q to quit, c to continue without paging--
Reading symbols from ./debug/mutool...
[New LWP 2323265]
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Core was generated by `./debug/mutool clean ../../../../pdf_fuzz/mupdf-1.25.5-source/mutool/clean/analy'.
Program terminated with signal SIGSEGV, Segmentation fault.

```

```

#0 0x00006285c5d0aaa0 in pdf_get_xref_entry_aux (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, i=6, solidify_if_needed=1)
    at source/pdf/pdf-xref.c:375
375                                     entry = &sub->table[i - sub->start];
(gdb) bt
#0 0x00006285c5d0aaa0 in pdf_get_xref_entry_aux (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, i=6, solidify_if_needed=1)
    at source/pdf/pdf-xref.c:375
#1 0x00006285c5d0aa878 in pdf_get_xref_entry (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, i=6)
    at source/pdf/pdf-xref.c:451
#2 0x00006285c5d0d3f0 in pdf_cache_object (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, num=6)
    at source/pdf/pdf-xref.c:2542
#3 0x00006285c5d0d0fe in pdf_resolve_indirect (ctx=0x6285e2c9c2a0, ref=0x6285e2cc81a0) at source/pdf/pdf-xref.c:2687
#4 0x00006285c5d0e422 in pdf_resolve_indirect_chain (ctx=0x6285e2c9c2a0, ref=0x6285e2cc81a0)
    at source/pdf/pdf-xref.c:2716
#5 0x00006285c5cc210d in pdf_is_dict (ctx=0x6285e2c9c2a0, obj=0x6285e2cc81a0) at source/pdf/pdf-object.c:344
#6 0x00006285c5c86c6f in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
    page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:232
#7 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
    page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9602d8, plast=0x7ffeba9602d0)
    at source/pdf/pdf-clean-file.c:175
#8 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
    page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#9 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
    page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9603d8, plast=0x7ffeba9603d0)
    at source/pdf/pdf-clean-file.c:175
#10 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
    page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#11 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
    page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9604d8, plast=0x7ffeba9604d0)
    at source/pdf/pdf-clean-file.c:175
#12 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
    page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#13 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
    page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9605d8, plast=0x7ffeba9605d0)
--Type <RET> for more, q to quit, c to continue without paging--

```

```
#1028 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#1029 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9801d8, plast=0x7ffeba9801d0)
at source/pdf/pdf-clean-file.c:175
#1030 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#1031 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9802d8, plast=0x7ffeba9802d0)
at source/pdf/pdf-clean-file.c:175
#1032 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
page_count=0, page_object_nums=0x0, names_list=0x0) at source/pdf/pdf-clean-file.c:239
#1033 0x00006285c5c86eed in strip_outline (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc81a0,
page_count=0, page_object_nums=0x0, names_list=0x0, pfirst=0x7ffeba9803d8, plast=0x7ffeba9803d0)
at source/pdf/pdf-clean-file.c:175
#1034 0x00006285c5c86ce9 in strip_outlines (ctx=0x6285e2c9c2a0, doc=0x6285e2cb6880, outlines=0x6285e2cc7f80,
```